

REMARKS

Claims 1-15 stand rejected under 35 U.S.C. §103 as being unpatentable over United States Patent Application Publication No. 2004/0131183 to Sako. Applicant respectfully traverses this rejection.

Applicant respectfully submits that the cited reference fails to disclose or suggest all of the claimed features of the present invention. More specifically, the Sako reference fails to disclose or suggest a magnetic disk apparatus that includes, *inter alia*, a cipher key memory unit that “stores a single cipher key used for encoding and decoding data” and a cipher key change unit that “cancels said cipher key stored in said cipher key memory unit and changes the data encoded and stored in the record medium into another key which cannot be decoded,” as now recited in amended independent Claim 1. Similarly, Applicants respectfully submit that the Sako reference fails to disclose or suggest a processing method that includes, *inter alia*, “a cipher key memory step of storing in a cipher key memory unit a single cipher key used for encoding and decoding data,” and “a cipher key change step of cancelling said cipher key stored in said cipher key memory unit and changing the data encoded and stored in a record medium into another cipher key which cannot be decoded,” as now recited in amended independent Claims 12 and 14.

In the present invention of independent Claims 1, 12 and 14, there is a cipher key that is stored in a cipher key memory unit. There is also a cipher key change unit that cancels the cipher key stored in the cipher key memory unit, and changes the data encoded and stored into another cipher key, where this changed data cannot be decoded. By changing

the cipher key that corresponds to data that has already been stored, it makes it impossible to decipher the stored data. Such a change in the cipher key is used, for example, when discarding or re-selling a computer in order to prevent a new user from accessing the previous owner's data, while still allowing the recording medium to be used by the new user.

More specifically, in the invention of independent Claims 1, 12 and 14, data is encoded into the record medium by encoding the data by use of a cipher key, and the data is decoded by use of the same cipher key by reading out the encoded data from the record medium. The record medium that has the encoded data recorded thereon is the same as the record medium from which the encoded data is to be read out, and the cipher key used for encoding is the same as the cipher key used for decoding. The encoded and recorded data can therefore be read out and decoded as long as the record medium is not destroyed.

However, when the user desires to cancel all of the data, the cipher key change unit is directed to cancel the cipher key stored in the memory unit, and replace it with a new cipher key. Thus, decoding of the encoded data recorded in the record medium becomes impossible because the cipher key has been changed. Accordingly, at this point in time, the recorded data is lost (such as would be desired by the user when discarding the computer).

In contrast, in the device of Sako, the encoded data is entered into the system via input terminal 11 (from the internet or other means), and it is decoded within deciphering circuit 12 by means of a cipher key. The decoded data then passes to watermark detection circuit 14, where copyright management data is detected, and, if the copyright detection management data permits it, the data is either directly recorded onto medium 16, or it is

recorded onto medium 16 after being encrypted with another cipher key that can be different from that used by deciphering circuit 12.

Thus, in Sako, the medium (or means) into which the encoded data is to be entered (terminal 11) is different from the medium that is ultimately used for recording (medium 16). If, therefore, even if the second phase of encoding and decoding is accomplished by using a cipher key that is different from the cipher key used for the first phase of decoding, the entered original data and the cipher keys used for decoding remain in existence, and thus the data is not lost in the device of Sako.

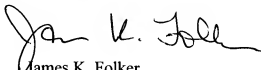
In other words, in Sako, there are two different cipher keys that are used in two different phases. In contrast, in the present invention of Claims 1, 12 and 14, there is a single cipher key that is changed after the data has been recorded. Changing the cipher key after recording the data purposely makes the data impossible to retrieve, which is the desired result when, for example, the user wants to discard the computer. Accordingly, as all of the claimed features of the present invention are not disclosed or suggested in the Sako et al. reference, Applicant respectfully requests the withdrawal of this §103 rejection of independent Claims 1, 12 and 14 and associated dependent Claims 2-11, 13 and 15.

For all of the above reasons, Applicant requests reconsideration and allowance of the claimed invention. Should the Examiner be of the opinion that a telephone conference

would aid in the prosecution of the application, or that outstanding issues exist, the Examiner is invited to contact the undersigned attorney.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By 
James K. Folker
Registration No. 37,538

September 9, 2008

Suite 2500
300 South Wacker Drive
Chicago, Illinois 60606
(312) 360-0080

Customer No. 24978